UNIT-III

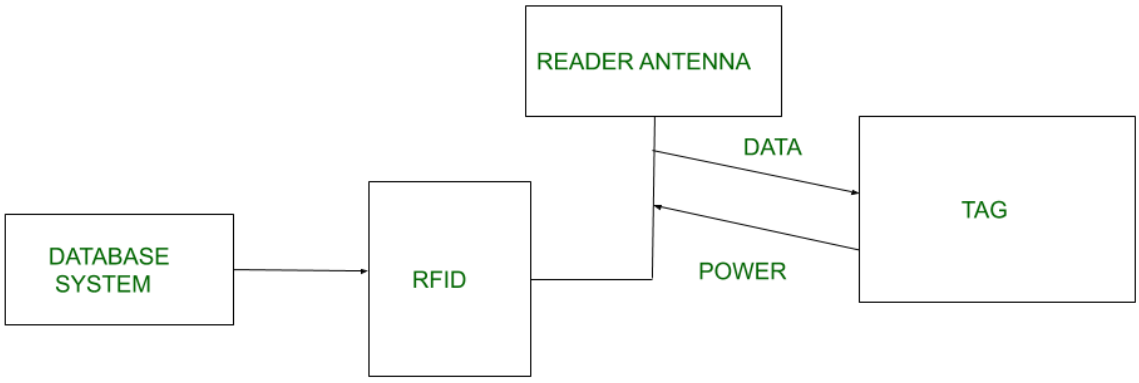
Four Pillars of IOT Paradigm

Radio Frequency Identification (RFID)

Radio Frequency Identification – or RFID – is used to automatically identify an object and capturing data about that object that has been stored in a small microchip tag and attached to the object.

RFID is a wireless system comprised of two components: tags and readers. The reader is a device that has one or more antennas that emit radio waves and receive signals back from the RFID tag. The RFID tag has a built-in antenna that communicates to a scanning device that reads the data remotely. The data is then transferred from the scanning device to the enterprise application software that houses the data. Each RFID tag has its own unique identifying number.

RFID can be used to record and control the movement of assets and personnel. You've probably seen RFID tags on the back of your library books, or even in the new biometric passports. It makes tracking assets contained in boxes or pallets easier to manage.



Working Principle of RFID:

An electronic RFID-enabled device can communicate with another RFID-enabled device. The device with which you want to establish a connection must be equipped with an RFID tag that will identify the electromagnetic waves transmitted by the RFID reader.

With the help of the technology, we can connect two RFID-enabled devices, one is the RFID reader and another is an electronic device designed with an RFID tag. Some RFID readers are designed with inbuilt RFID antennas and some of them come with antenna ports. The users need to include separate antennas to make the readers work.

Once the RFID reader is activated, it will start generating radio-frequency signals and when the reader's antennas are within the specified range covered by the RFID tag of another RFID-enabled device, the reader will decode the electronic information stored in the RFID tag. This is how RFID readers can identify and decode electronic data and ensure a secure data exchange process.

The components of RFID

Using radio waves and electromagnetic fields to send data, an RFID tag and the system that reads it consists of three main components.

Component #1 – the RFID tag: there are two types of RFID tags, passive and active. A passive RFID tag is the barcode you see in the supermarket. It is assigned to an item, it is easy to activate, and it does not have a power supply. An active RFID tag, like the sensor tag in the back of a library book, has a microchip that collects information about the asset and may also contain an antenna or on-board sensor.

Component #2 – the RFID reader: An RFID reader is a device that scans the RFID tag and collects information about the asset the tag is attached to. These readers can be hand-held or wired, and work with USB and Bluetooth. Not all barcode scanners can read an RFID tag, but all RFID readers can read a barcode.

Component #3 – the RFID applications or software: this software controls and monitors the RFID tags that have been attached to your assets. It can be a mobile application or a standard software package. Most of the time you can find RFID

software that has a mobile application that works in conjunction with it. This software can communicate with the reader using Bluetooth or Beacon technology.

Features of RFID:

- An RFID tag consists of two-part which is a microcircuit and an antenna.
- This tag is covered by protective material which acts as a shield against the outer environment effect.
- This tag may active or passive in which we mainly and widely used passive RFID.

Application of RFID:

- It utilized in tracking shipping containers, trucks and railroad, cars.
- It uses in Asset tracking.
- It utilized in credit-card shaped for access application.
- It uses in Personnel tracking.
- Controlling access to restricted areas.
- It uses ID badging.
- Supply chain management.
- Counterfeit prevention (e.g., in the pharmaceutical industry).

Advantages of RFID:

- It provides data access and real-time information without taking too much time.
- RFID tags follow the instruction and store a large amount of information.
- The RFID system is non-line of sight nature of the technology.
- It improves the Efficiency, traceability of production.
- In RFID hundreds of tags read in a short time.

Disadvantages of RFID:

- It takes longer to program RFID Devices.
- RFID intercepted easily even it is Encrypted.
- In an RFID system, there are two or three layers of ordinary household foil to dam the radio wave.
- There is privacy concern about RFID devices anybody can access information about anything.
- Active RFID can costlier due to battery.

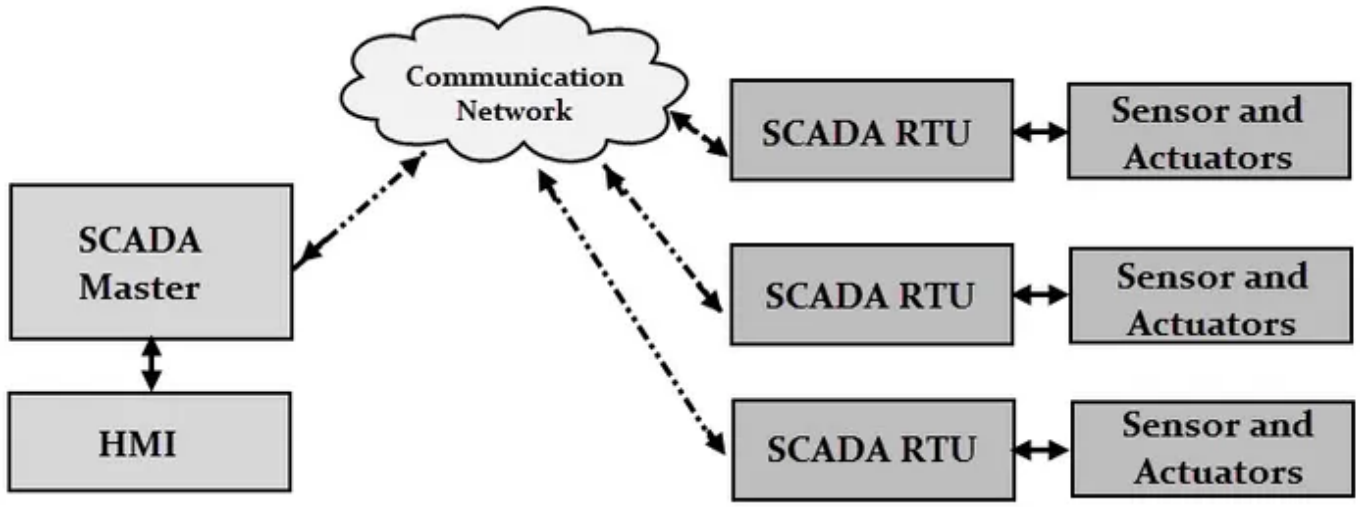
SCADA--Supervisory Control and Data Acquisition

SCADA stands for “Supervisory Control and Data Acquisition”. SCADA is a type of process control system architecture that uses computers, networked data communications and graphical Human Machine Interfaces (HMIs) to enable a high-level process supervisory management and control.

SCADA systems communicate with other devices such as programmable logic controllers (PLCs) and PID controllers to interact with industrial process plant and equipment.

SCADA systems form a large part of control systems engineering. SCADA systems gather pieces of information and data from a process that is analyzed in real-time (the “DA” in SCADA). It records and logs the data, as well as representing the collected data on various HMIs.

This enables process control operators to supervise (the “S” in SCADA) what is going on in the field, even from a distant location. It also enables operators to control (the “C” in SCADA) these processes by interacting with the HMI.

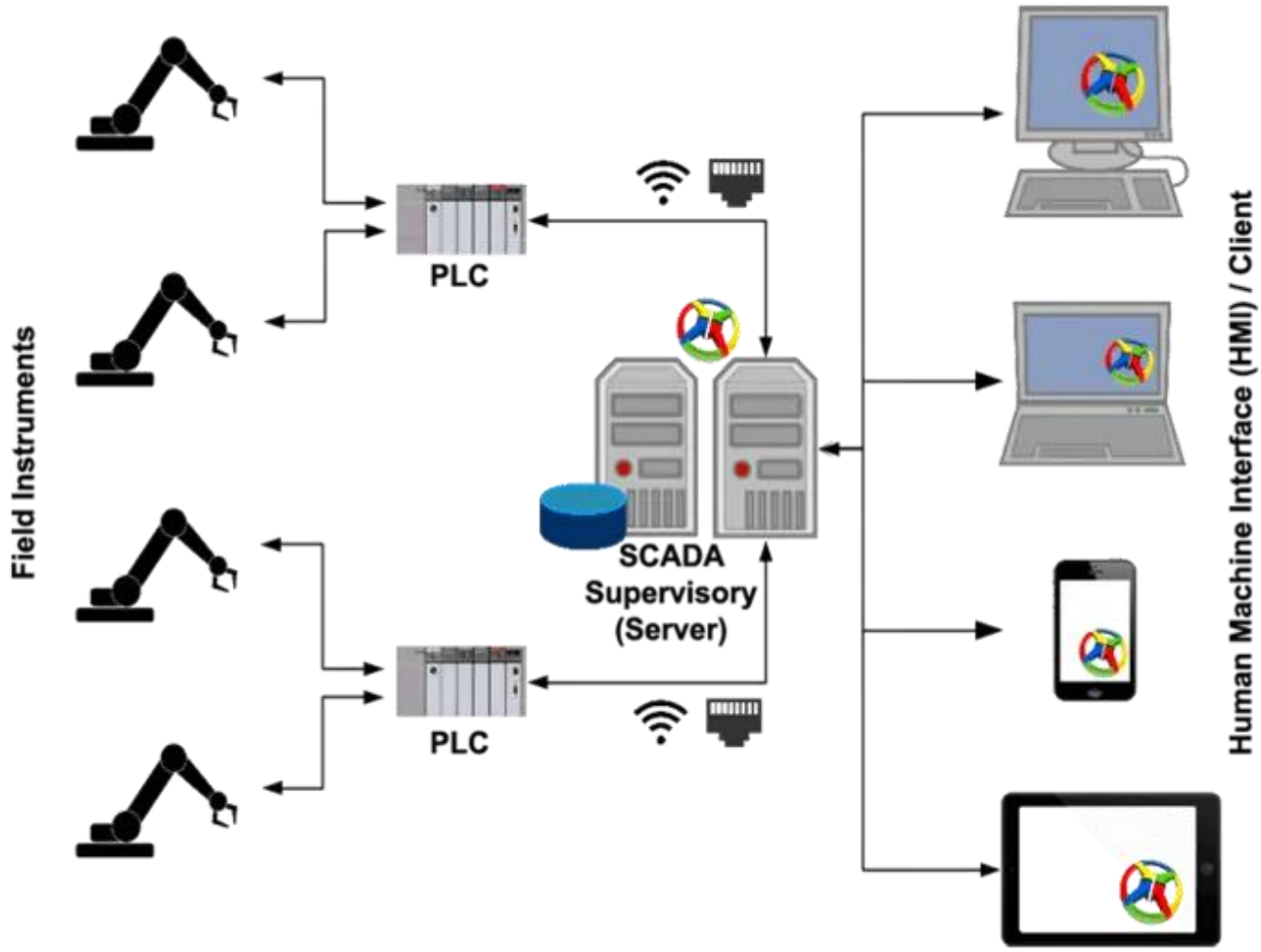


Generic SCADA System

Supervisory Control and Data Acquisition systems are essential to a wide range of industries and are broadly used for the controlling and monitoring of a process. SCADA systems are prominently used as they have the power to control, monitor, and transmit data in a smart and seamless way. In today’s data-driven world, we are always looking for ways to increase automation and make smarter decisions through the proper use of data – and SCADA systems are a great way of achieving this.

SCADA systems can be run virtually, which allows the operator to keep a track of the entire process from his place or control room. Time can be saved by using SCADA efficiently.

One such excellent example is, SCADA systems are used extensively in the Oil and Gas sector. Large pipelines will be used to transfer oil and chemicals inside the manufacturing unit. Hence, safety plays a crucial role, such that there should not be any leakage along the pipeline. In case, if some leakage occurs, a SCADA system is used to identify the leakage. It infers the information, transmits it to the system, displays the information on the computer screen and also gives an alert to the operator.



SCADA Architecture

Generic SCADA systems contain both hardware and software components. The computer used for analysis should be loaded with SCADA software. The

hardware component receives the input data and feds it into the system for further analysis.

SCADA system contains a hard disk, which records and stores the data into a file, after which it is printed as when needed by the human operator. SCADA systems are used in various industries and manufacturing units like Energy, Food and Beverage, Oil and Gas, Power, Water, and Waste Management units and many more.

Features of SCADA systems

Although SCADA systems may include special features for specific industries or applications, most systems support the following features:

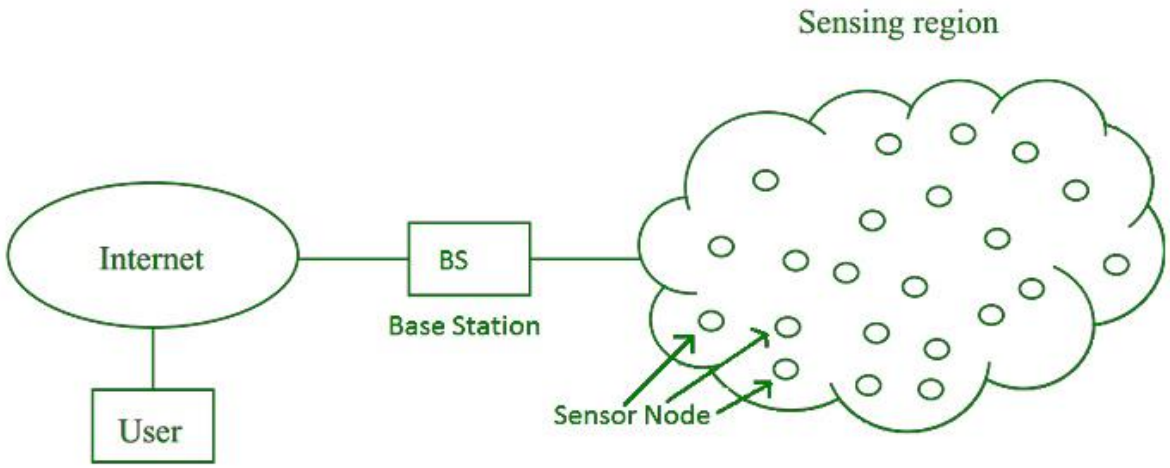
- **Data acquisition** is a foundation of SCADA systems; sensors collect data and deliver it to field controllers, which, in turn, feed data to the SCADA computers.
- **Remote control** is achieved through the control of field actuators, based on the data acquired from field sensors.
- **Networked data communication** enables all SCADA functions. Data collected from sensors must be transmitted to SCADA field controllers, which, in turn, communicate with the SCADA supervisory computers; remote control commands are transmitted back to actuators from the SCADA supervisory computers.
- **Data presentation** is achieved through HMIs, which represent current and historical data to the operators running the SCADA system.
- **Real-time and historical data** are both important parts of the SCADA system, as they enable users to track current performance against historical trends.
- **Alarms** alert SCADA operators to potentially significant conditions in the system. Alerts can be configured to notify operators when processes are blocked, when systems are failing, or when other aspects of SCADA processes need to be stopped, started or adjusted.
- **Reporting** on SCADA system operations can include reports on system status, process performance and reports customized to specific uses.

Wireless Sensor Network (WSN)

Wireless Sensor Network (WSN) is an infrastructure-less wireless network that is deployed in a large number of wireless sensors in an ad-hoc manner that is used to monitor the system, physical or environmental conditions.

Sensor nodes are used in WSN with the onboard processor that manages and monitors the environment in a particular area. They are connected to the Base Station which acts as a processing unit in the WSN System.

Base Station in a WSN System is connected through the Internet to share data.



WSN can be used for processing, analysis, storage, and mining of the data.

Applications of WSN:

1. Internet of Things (IOT)
2. Surveillance and Monitoring for security, threat detection
3. Environmental temperature, humidity, and air pressure
4. Noise Level of the surrounding
5. Medical applications like patient monitoring
6. Agriculture
7. Landslide Detection

Challenges of WSN:

1. Quality of Service
2. Security Issue
3. Energy Efficiency
4. Network Throughput

5. Performance
6. Ability to cope with node failure
7. Cross layer optimisation
8. Scalability to large scale of deployment

Components of WSN:

1. **Sensors:**
   Sensors in WSN are used to capture the environmental variables and which is used for data acquisition. Sensor signals are converted into electrical signals.
2. **Radio Nodes:**
   It is used to receive the data produced by the Sensors and sends it to the WLAN access point. It consists of a microcontroller, transceiver, external memory, and power source.
3. **WLAN Access Point:**
   It receives the data which is sent by the Radio nodes wirelessly, generally through the internet.
4. **Evaluation Software:**
   The data received by the WLAN Access Point is processed by a software called as Evaluation Software for presenting the report to the users for further processing of the data which can be used for processing, analysis, storage, and mining of the data.

Types of Communications in IOT

IOT Communication :

IoT is connection of devices over internet, where these smart devices communicate with each other , exchange data , perform some tasks without any human involvement. These devices are embedded with electronics, software, network and sensors which help in communication. Communication between smart devices is very important in IOT as it enables these devices to gather, exchange data which contribute in success of that IOT product/project.

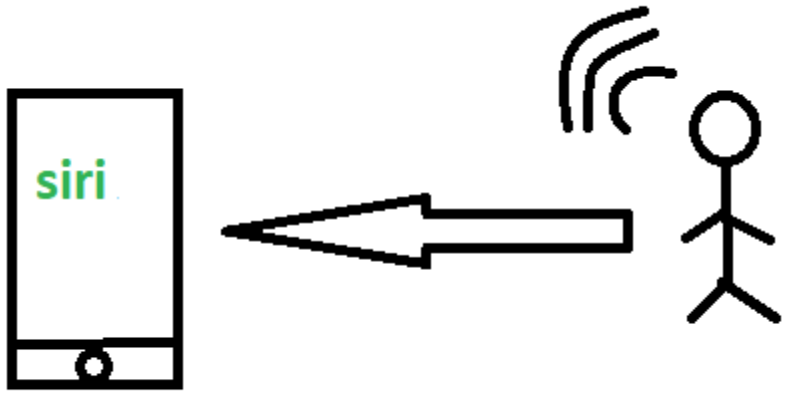
Types of Communications in IOT :

The following are some communication types in IoT:-

1. **Human to Machine (H2M) :**

   In this human gives input to IOT device i.e as speech/text/image etc. IOT device (Machine) like sensors and actuators then understands input, analyses it and responds back to human by means of text or Visual Display. This is very useful as these machines assist humans in every everyday tasks. It is a

combo of software and hardware that includes human interaction with a machine to perform a task.



H2M communication

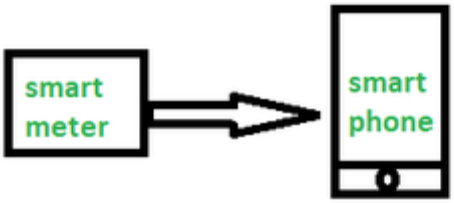
Merits: This H2M has a user-friendly interface that can be quickly accessed by following the instructions. It responds more quickly to any fault or failure. Its features and functions can be customized.

Examples:

- Facial recognition.
- Bio-metric Attendance system.
- Speech or voice recognition.

2. **Machine to Machine (M2M):**

   In this the interaction or communication takes place between machines by automating data/programs. In this machine level instructions are required for communication. Here communication takes place without human interaction. The machines may be either connected through wires or by wireless connection. An M2M connection is a point-to-point connection between two network devices that helps in transmitting information using public networking technologies like Ethernet and cellular networks. IoT uses the basic concepts of M2M and expands by creating large “cloud” networks of devices that communicate with one another through cloud networking platforms.



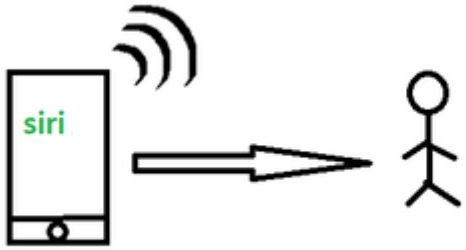
M2M communication

Advantages –
This M2M can operate over cellular networks and is simple to manage. It can be used both indoors and outdoors and aids in the communication of smart objects without the need for human interaction. The M2M contact facility is used to address security and privacy problems in IoT networks. Large-scale data collection, processing, and security are all feasible.
Disadvantages –
However, in M2M, use of cloud computing restricts versatility and creativity. Data security and ownership are major concerns here. The challenge of achieving interoperability between cloud/M2M IoT systems is daunting. M2M connectivity necessitates the existence of a reliable internet connection.
Examples:

- Smart Washing machine sends alerts to the owners' smart devices after completion of washing or drying of clothes.
- Smart meters tracks amount of energy used in household or in companies and automatically alert the owner.

3. **Machine to Human (M2H) :**

   In this machine interacts with Humans. Machine triggers information (text messages/images/voice/signals) respective / irrespective of any human presence. This type of communication is most commonly used where machines guide humans in their daily life. It is way of interaction in which humans co-work with smart systems and other machines by using tools or devices to finish a task.



M2H communication

Examples:

- Fire Alarms
- Traffic Light
- Fitness bands
- Health monitoring devices

4. Human to Human (H2H) :
This is generally how humans communicate with each other to exchange information by speech, writing, drawing, facial expressions, body language

etc. Without H2H, M2M applications cannot produce the expected benefits unless humans can immediately fix issues, solve challenges, and manage scenarios.

H2H communication

For, communication of IoT devices many protocols are used. These IoT protocols are modes of communication which give security to the data being exchanged between IoT connected devices. Example bluetooth, wifi, zigbee etc.

Internet of Things (IoT) Enabling Technologies

IoT (internet of things) enabling technologies are

1. Wireless Sensor Network
2. Cloud Computing
3. Big Data Analytics
4. Communications Protocols
5. Embedded System

1. Wireless Sensor Network (WSN) :

A **WSN** comprises distributed devices with sensors which are used to monitor the environmental and physical conditions. A **wireless sensor network** consists of end nodes, routers and coordinators. End nodes have several sensors attached to them where the data is passed to a coordinator with the help of routers. The coordinator also acts as the gateway that connects WSN to the internet.

Example –

- Weather monitoring system
- Indoor air quality monitoring system
- Soil moisture monitoring system
- Surveillance system
- Health monitoring system

2. Cloud Computing :

It provides us the means by which we can access applications as utilities over the internet. Cloud means something which is present in remote locations.

With Cloud computing, users can access any resources from anywhere like databases, webservers, storage, any device, and any software over the internet.

Characteristics –

1. Broad network access
2. On demand self-services
3. Rapid scalability
4. Measured service
5. Pay-per-use

Provides different services, such as –

- **IaaS (**Infrastructure as a service**)**
  Infrastructure as a service provides online services such as physical machines, virtual machines, servers, networking, storage and data center space on a pay per use basis. Major IaaS providers are Google Compute Engine, Amazon Web Services and Microsoft Azure etc.
  Ex : Web Hosting, Virtual Machine etc.
- **PaaS (**Platform as a service**)**
  Provides a cloud-based environment with a very thing required to support the complete life cycle of building and delivering West web based (cloud) applications – without the cost and complexity of buying and managing underlying hardware, software provisioning and hosting. Computing platforms such as hardware, operating systems and libraries etc. Basically, it provides a platform to develop applications.
  Ex : App Cloud, Google app engine
- **SaaS (**Software as a service**)**
  It is a way of delivering applications over the internet as a service. Instead of installing and maintaining software, you simply access it via the internet, freeing yourself from complex software and hardware management.
  SaaS Applications are sometimes called web-based software on demand software or hosted software.
  SaaS applications run on a SaaS provider's service and they manage security availability and performance.
  Ex : Google Docs, Gmail, office etc.

3. Big Data Analytics :

It refers to the method of studying massive volumes of data or big data. Collection of data whose volume, velocity or variety is simply too massive and tough to store, control, process and examine the data using traditional databases.

Big data is gathered from a variety of sources including social network videos, digital images, sensors and sales transaction records.

Several steps involved in analyzing big data –

1. Data cleaning
2. Munging
3. Processing
4. Visualization

Examples –

- Bank transactions
- Data generated by IoT systems for location and tracking of vehicles
- E-commerce and in Big-Basket
- Health and fitness data generated by IoT system such as a fitness bands

4. Communications Protocols :

They are the backbone of IoT systems and enable network connectivity and linking to applications. Communication protocols allow devices to exchange data over the network. Multiple protocols often describe different aspects of a single communication. A group of protocols designed to work together is known as a protocol suite; when implemented in software they are a protocol stack.

They are used in

1. Data encoding
2. Addressing schemes

5. Embedded Systems:

It is a combination of hardware and software used to perform special tasks. It includes microcontroller and microprocessor memory, networking units (Ethernet Wi-Fi adapters), input output units (display keyword etc.) and storage devices (flash memory).

It collects the data and sends it to the internet.

Embedded systems used in

Examples –

1. Digital camera
2. DVD player, music player
3. Industrial robots
4. Wireless Routers etc.

IoT Levels- Deployment Templates

Developing an **IoT Level Template** system consists of the following components:

1. **Device:** These may be sensors or actuators capable of identifying, remote sensing, or monitoring.
2. **Resources:** These are software components on IoT devices for accessing and processing. storing software components or controlling actuators

connected to the device. Resources also include software components that enable network access.

3. **Controller Service:** It is a service that runs on the device and interacts with web services. The controller service sends data from the device to the web service and receives commands from the application via web services for controlling the device.
4. **Database:** Stores data generated from the device
5. **Web Service:** It provides a link between IoT devices, applications, databases, and analysis components.
6. **Analysis Component:** It performs an analysis of the data generated by the lol device and generates results in a form which are easy for the user to understand.
7. **Application:** It provides a system for the user to view the system status and view product data. It also allows users to control and monitor various aspects of the IoT system.

IoT Levels

IoT level 1

IoT systems have a single device that performs sensing or actuation, stores a. analyses it and hosts the application, IoT system-level-l is the best example for modeling low complexity and low-cost solution where the analysis requirement is hok comprehensive and data involved is not big.

Example: We can understand with the help of an eg. let's look at the IoT device that monitors the lights in a house. The lights are controlled through switches. The database has maintained the status of each light and also REST services deployed locally allow retrieving and updating the state of each light and trigger the switches accordingly. For controlling the lights and applications, the application has an interface. The device is connected to the internet and hence the application can be accessed remotely as well.

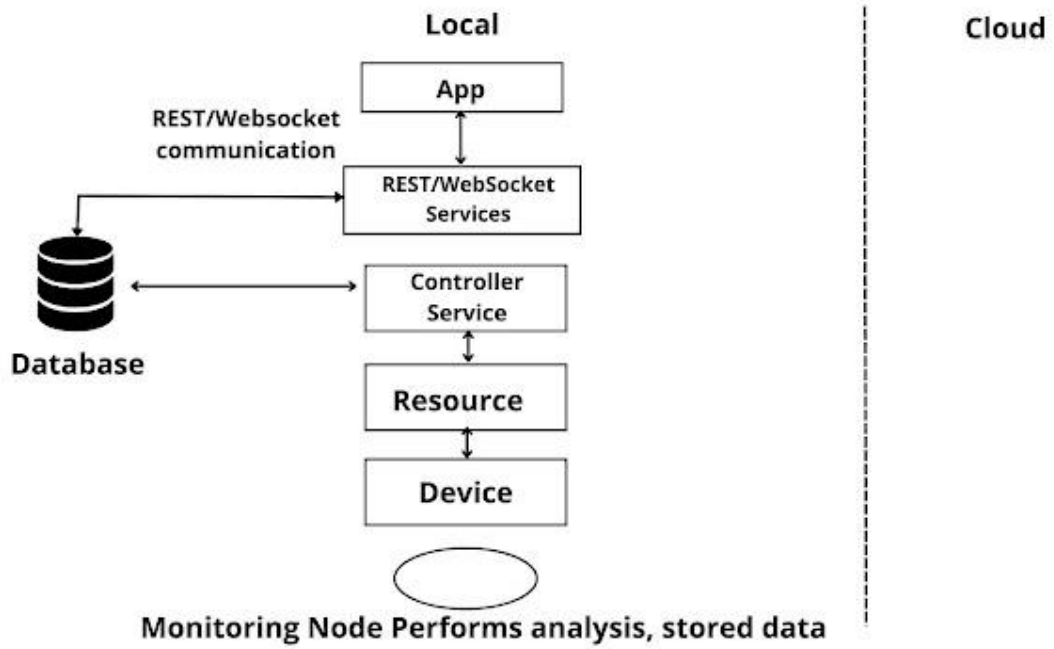


Fig. **IoT Level-1**

IoT level 2

A node performs sensing/actuation and local analysis. Data is stored in the cloud. this level is facilitated where the data involved is big and primary analysis is not comprehensive

Example: Cloud-based application is used for monitoring and controlling the IoT system A single node monitors the soil moisture in the field Which is sent to the database on the cloud using REST APIS. The controller service continuously monitors moisture levels.

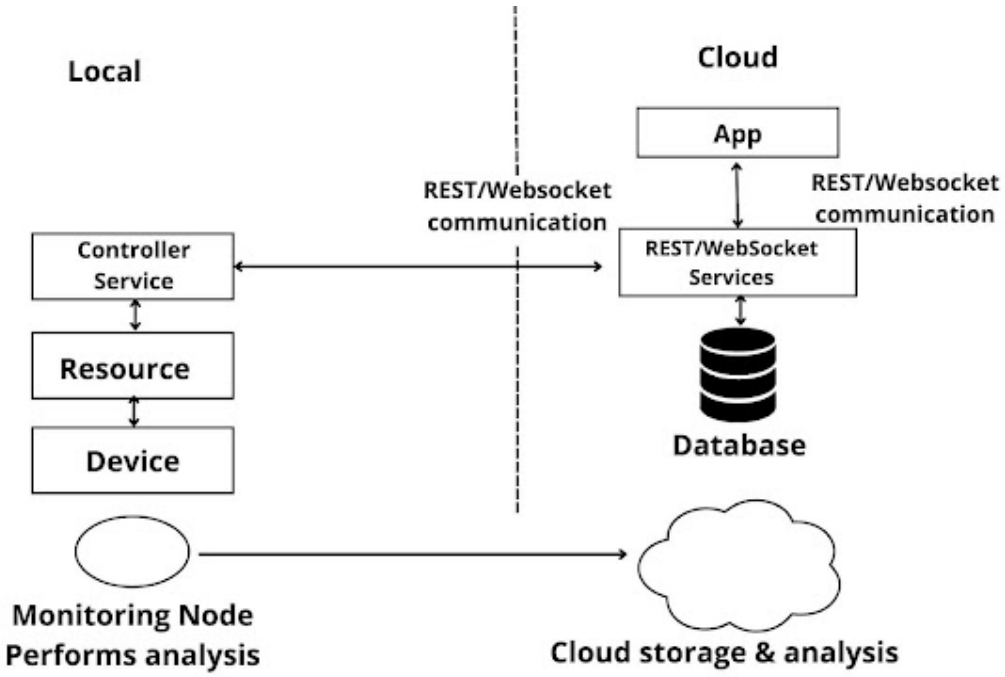


Fig. **IoT Level-2**

IoT level 3

At this level, the application is cloud-based. A single node monitors the environment and stores data in the cloud. This is suitable where data is comprehensive and analysis 1 computationally intensive.

Example: A node is monitoring a package using devices like an accelerometer and gyroscope. These devices track vibration levels. controller service sends sensor data to the cloud in the rear time using WebSocket APL. Data is stored in the cloud and visualized using a cloud-based application. The analysis component triggers an alert if vibration levels cross a threshold.

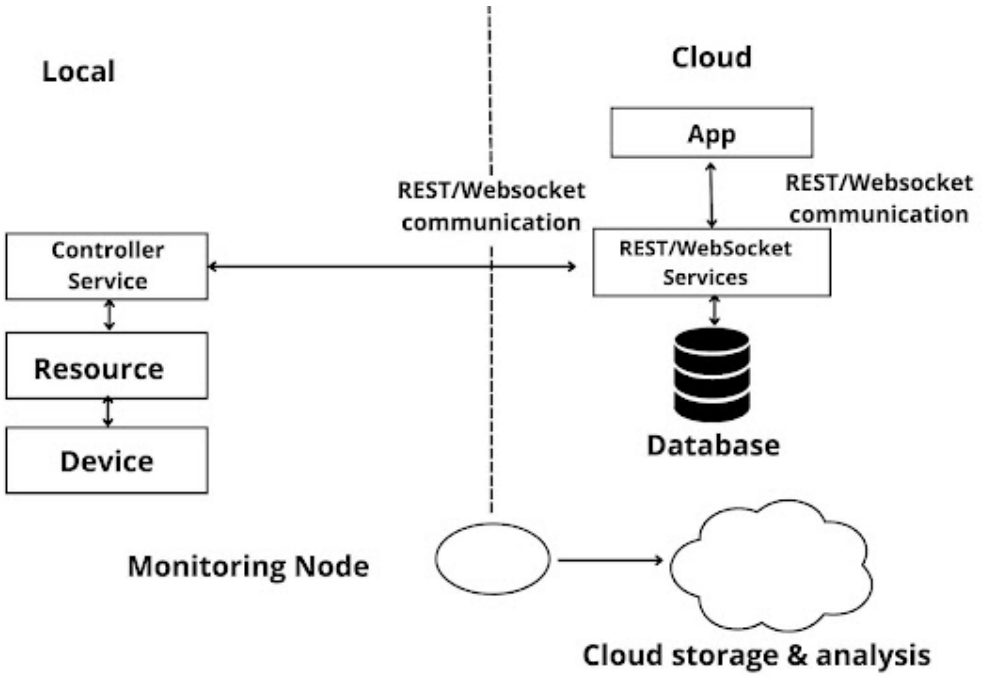


Fig. **IoT Level-3**

IoT level 4

At this level, Multiple nodes collect information and store it in the cloud. Local and rent server nodes are used to grant and receive information collected in the cloud from various devices. Observer nodes can process information and use it for applications but not perform control functions, This level is the best solution where data involvement is big, requirement analysis is comprehensive and multiple nodes are required,

Example: Analysis is done on the cloud and the entire IoT system has monitored the cloud using an application. Noise monitoring of an area requires various nodes to function independently of each other. Each has its own controller service. Data is stored in a cloud database.

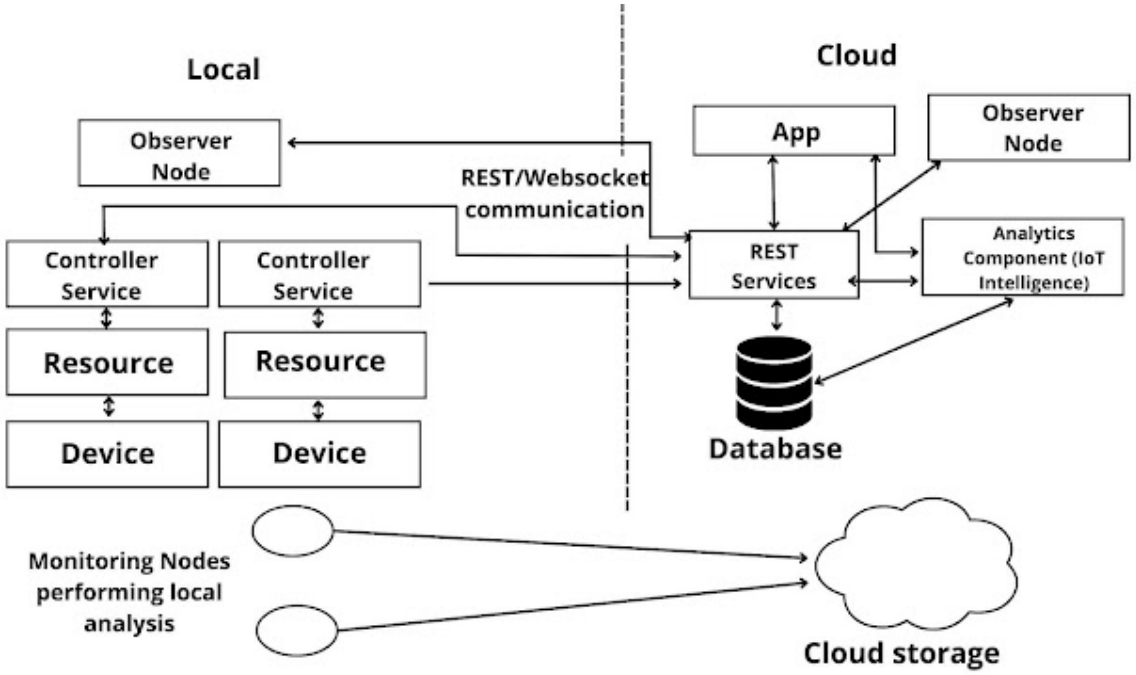


Fig. **IoT Level-4**

IoT level 5

In this level Nodes present locally are of two types end odes and coordinator nodes End nodes collect data and perform sensing or actuation or both. Coordinator nodes collect data from end nodes and send it to the cloud. Data is stored and analyzed in the cloud. This level is best for WSN, where the data involved is big and the requirement analysis is comprehensive.

Example: A monitoring system has various components: end nodes collect various data from the environment and send it to the coordinator node. The coordinator node acts as a gateway and allows the data to be transferred to cloud storage using REST API. The controller service on the coordinator node sends data to the cloud.

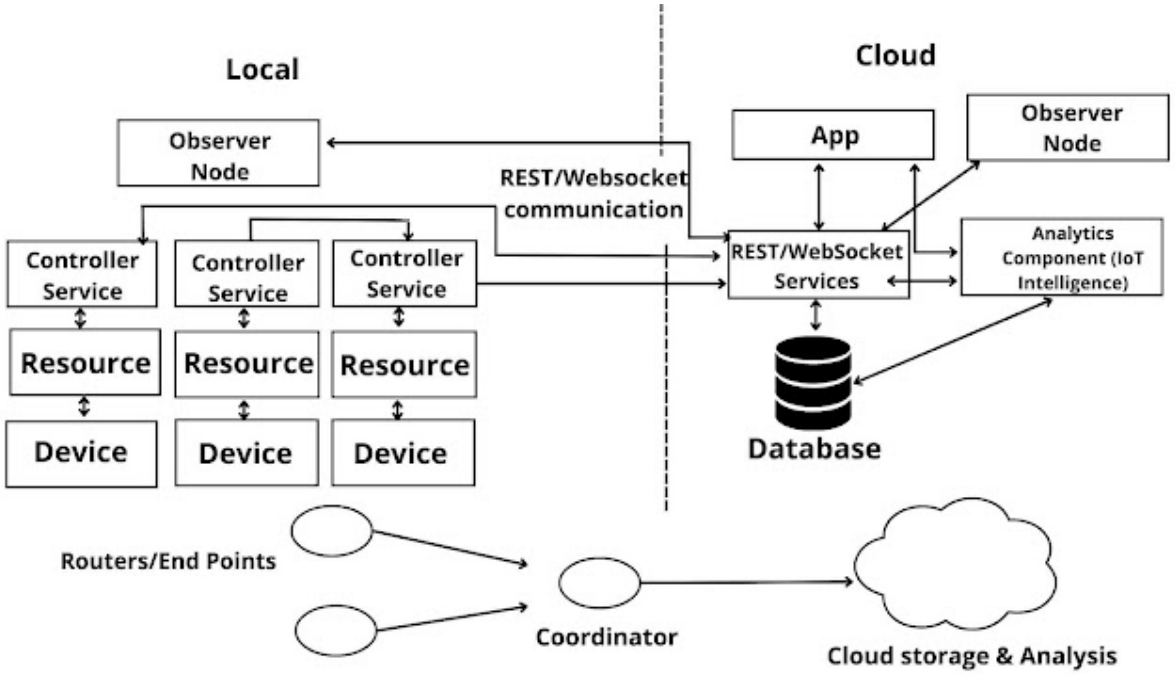


Fig. **IoT Level-5**

IoT Level-6

At this level, the application is also cloud-based and data is stored in the cloud-like of levels. Multiple independent end nodes perform sensing and actuation and send d to the cloud. The analytics components analyze the data and store the results in the cloud database. The results are visualized with a cloud-based application. The centralized controller is aware of the status of all the end nodes and sends control commands to the nodes.

Example: Weather monitoring consists of sensors that monitor different aspects of the system. The end nodes send data to cloud storage. Analysis of components, applications, and storage areas in the cloud. The centralized controller controls all nodes and provides inputs.

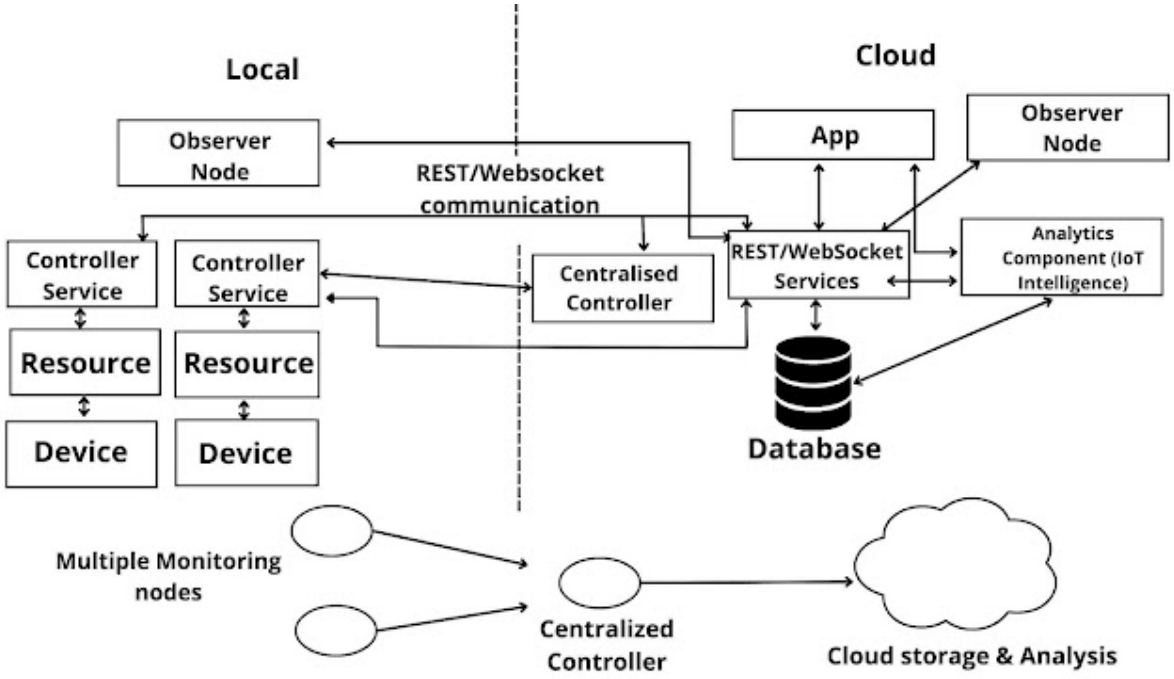


Fig. **IoT Level-6**